

ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE TECNOLOGÍA DE LA TSA "AUTORIDAD DE ESTAMPADO O SELLADO DE TIEMPO" PARA LA INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI, FIRMA DIGITAL) Y SOFTWARE PARA EL CORRESPONDIENTE DESPLIEGUE DE CERTIFICADOS DE ACUERDO CON LOS CRITERIOS ESPECÍFICOS DE ACREDITACIÓN EXIGIDOS POR LA ONAC PARA SER IMPLEMENTADA EN LA POLICÍA NACIONAL.//PROCUREMENT, INSTALLATION AND COMMISSIONING TECHNOLOGY TSA "AUTHORITY STAMPING OR TIME STAMP" FOR THE PUBLIC KEY INFRASTRUCTURE (PKI, DIGITAL SIGNATURE) AND THE CORRESPONDING SOFTWARE DEPLOYMENT CERTIFICATES ACCORDING TO THE SPECIFIC CRITERIA REQUIRED FOR ACCREDITATION BY ONAC TO BE IMPLEMENTED IN THE NATIONAL POLICE.

DESCRIPCION // DESCRIPTION

Entrega detallado del cronograma de ejecucion del proyecto // Delivery detailed schedule of project implementation

Objetivo general: Fortalecimiento de la plataforma tecnologica que permita obtener la acreditación como entidad CDF cerrada (entidad certificadora de documentos y firmas) a la Policía Nacional, para el control y la seguridad de la informacion
Objetivos específicos: El contratista instalara una infraestructura de llave pública (PKI) de acuerdo a los criterios específicos de acreditación exigidos por ONAC.//Objective: Strengthening the technological platform to gain accreditation as a closed entity CDF (certification authority documents and signatures) to the National Police for the control and safety information specific Objectives: The contractor shall install a public key infrastructure (PKI) according to specific criteria required for accreditation ONAC.

El contratista implementar una autoridad de estampado cronológico, equipo TSA, de acuerdo a las siguientes especificaciones técnicas:

CARACTERÍSTICAS:

- Protocolo de sellado de tiempo HTTP siguiendo estándar RFC3161.
- El oferente entregara administración del sistema vía HTTPS con requerimiento de certificado de operador.
- Generación de claves privadas RSA, desde 1024 hasta 2048 bits.
- Generación de peticiones de certificados desde un dispositivo acreditado de forma segura.
- Configuración del servicio de sellado de tiempo, donde se provee la creación de la clave privada del certificado TSA de forma segura, así como la importación del certificado digital asociado dentro del dispositivo criptográfico integrado en la solución TSA(HSM).
- Capacidad total de configuración del sistema: dirección de red, inicialización de dispositivo criptográfico.

-Capacidad de configurar múltiples repositorios de fuentes de tiempo distribuidos en distintas zonas geográficas.

- Sincronización del reloj del sistema vía NTP. (Posibilidad de incorporación de otros sistemas de sincronismo: GPS).

- Servidor TSA formato appliance, con Hardware criptográfico integrado (HSM) certificado FIPS 140-2 Level 3 y Common Criteria EAL4+.

-Base de datos incluida en Solución de TSA Postgress, con posibilidad de utilizar otras bases de datos externas como Oracle y MySQL.

Características Mínimas Técnicas Servidor TSA Appliance:

-Formato Servidor 2U,CSE-825MTQ-7"W REDUNDANTE CHASIS 2U N,2 POWER SUPPLY - HOT SWAP

-HSM(Hardware Security Module) integrado en servidor de TSA

-Placa Base Single Socket, Procesador Xeon X3330@2,6,Intel IVY BRIDGE 4C E3-1220V2 3.1G 8M, RAM:8 GB DDR3 1333 UNBUFFERED ECC

-2 HDD RAID 1: SATA3 1TB WD1003FBYZ 6GB/S 7.2K 64 MB,

-Soporte Smart Card 2U Inferior V2, Soporte Smart Card 2U Intermedio V3, Guía Smart Smart Card V3

-SOPORTE DISCOS DUROS FIJOS 825MT-Q, DISPLAY 635 USB LCD 20X4+Y11, CBL-SATA CABLE ALIMENTACION, PLACA LECTOR LTC36 USB2 CIN CABLE DE CONEXIÓN USB,

-Cerradura de Contacto REA-11952/4, CIERRE USB Trasero, Riser Card 2U Pasivo, Cable Alimentación SATA Acodado

Diseño e implementación: TSA (Autoridad de estampado de tiempo) PONAL:

- Instalación y puesta en producción del sistema.

- Mantenimiento y soporte anual 8x5 . Dos años//

The contractor shall implement a chronological stamping authority, TSA team, according to the following specifications:

Features:

HTTP Protocol of sealing time following standard RFC3161.

-The Bidder deliver system administration via HTTPS with operator certificate requirement.

-generation RSA private key from 1024-2048 bits.

-generation Certificate request from an accredited device safely.

-Setting Time stamping service, where the creation of the private key of TSA certificate is provided safely and importing the digital certificate associated within the integrated TSA (HSM) solution cryptographic device.

Ability overall system configuration: network address, cryptographic device initialization.

Ability to configure multiple repositories time sources distributed in different geographical areas.

- Synchronize the system clock via NTP. (Ability to incorporate other sync systems: GPS).

- Server TSA appliance format with integrated cryptographic hardware (HSM) certified FIPS 140-2 Level 3 and Common Criteria EAL4 +.

-Database Included in Postgress TSA solution, with the possibility of using other external databases like Oracle and MySQL.

Minimum TSA Server Appliance Technical features:

-format Server 2U, CSE-825MTQ-7"W REDUNDANT N CHASSIS 2U, 2 POWER SUPPLY - HOT SWAP

-HSM (Hardware Security Module) integrated TSA server

-Placa Base Single Socket, Xeon X3330 Processor @ 2.6, Intel IVY BRIDGE 4C 3.1G E3-1220V2 8M RAM: 8 GB DDR3 1333 ECC UNBUFFERED

RAID 1 -2 HDD: 1TB SATA3 6GB WD1003FBYZ / S 7.2K 64MB

-Support Bottom 2U V2 Smart Card, Smart Card Support 2U Intermediate V3, V3 Smart Card Smart Guide

-Support HARD DRIVES FIXED 825MT-Q, 20X4 LCD DISPLAY 635 USB + Y11, CBL-SATA POWER CABLE, INC PLATE READER LTC36 USB2 USB CABLE CONNECTION,

-Lock Of Contacto REA-11952/4, CLOSE USB Rear, Riser Card 2U Passive, Right Angle SATA Power Cable

Design and Implementation: TSA (Time Stamping Authority) PONAL:

- Installation and commissioning production system.

- Maintenance and annual 8x5. // Two years

El contratista Implementara los ajustes tecnológicos necesarios a la PKI existente de la Policia Nacional para la puesta en marcha con la TSA, para el proceso de acreditacion y integracion con el GECOP " gestor de contenidos Policiales" , incluye:

Elaboración de la declaración de prácticas de certificación, DPC.

Programación de la Autoridad de Certificación, CA de Microsoft, para incluir los contenidos definidos en cada certificado digital.

Diseño del hardware para conseguir la ingeniería de disponibilidad requerida, tanto para la CA como para la CRL.

Definición de procesos administrativos de gestión de la CA y la RA (emisión, revocación y suspensión).

Programación de rutinas de gestión de certificados: Notificaciones.

El contratista configurar la respectiva firma digital en el GECOP "Gestor de contenidos Policiales".

El contratista colocara dos ingenieros en sitio para la puesta en marcha de la plataforma.

Una vez entregada la solución se debe brindar soporte por dos años de todo lo realizado.

// The contractor will implement the necessary technological adjustments to the existing PKI National Police for commissioning with the TSA, for the accreditation process and integration with GECOP "Police content manager" includes:

Preparation of certification practice statement, DPC.

Programming Certification Authority, CA Microsoft, to include the contents defined in each digital certificate.

Design of hardware to achieve the engineering required availability for both AC or the CRL.

Definition of administrative management processes CA and RA (issuance, revocation and suspension).

Scheduling certificate management routines: Notifications.

The contractor configure the respective digital signature on the GECOP "Police content manager".

The contractor placed two engineers on site for the launch of the platform.

Once delivered the solution must support two years everything done.

El contratista realizara los ajustes en la infraestructura PKI según requisitos de acreditación o los que se requieran para su perfecto funcionamiento:

- Elaboración de la declaración de prácticas de certificación, DPC.
- Programación de la Autoridad de Certificación, CA de Microsoft, para incluir los contenidos definidos en cada certificado digital.
- Diseño del hardware e implementación para conseguir la ingeniería de disponibilidad requerida, tanto para la CA como para la CRL.
- Definición de procesos administrativos de gestión de la CA y la RA (emisión, revocación y suspensión)
- Programación de rutinas de gestión de certificados: Notificaciones.
- Integración Tokens Dual Factor
- Soporte por un año de todo lo realizado con la plataforma.

//Implementing PKI infrastructure settings as requirements for accreditation or required for perfect operation:

- Development of certification practice statement, DPC.
- Programming Certification Authority, CA Microsoft, to include the contents defined in each digital certificate.
- Design and implementation of hardware engineering to get the required availability for both CA and for the CRL.
- Definition of administrative management processes CA and RA (issuance, revocation and suspension)
- Programming certificate management routines: Notifications.
- Integration Tokens Dual Factor
- Support for a year everything done with the platform.

El contratista Implementara los requisitos normativos de la ISO / IEC 17065 de 2012.// The contractor will implement the regulatory requirements of ISO / IEC 17065, 2012.

Ejecución Ethical HACKING, Informe y soluciones. //Ethical HACKING Execution Report and solutions.

EJECUTAR PRUEBAS DE VULNERABILIDADES EN LA INFRAESTRUCTURA DE LLAVES PÚBLICAS DE PONAL, DE ACUERDO A LAS SIGUIENTES DEFINICIONES:

El contratista Identificara, cuantificara, validara y valorar las principales vulnerabilidades presentes en la plataforma Tecnológica PKI; al igual que la ejecución de un test de penetración tipo White box a los principales sistemas de información y servicios de red que hacen parte de la infraestructura tecnológica de PKI, con el fin de validar las debilidades identificadas que podrían hacer inmanejable el nivel de riesgo y facilitar el compromiso de los procesos corporativos.

- Evaluación de vulnerabilidades la Seguridad de la Información con respecto al acceso lógico.
- Identificación de vulnerabilidades técnicas sobre los servidores de la organización.
- Realización de evaluación de vulnerabilidades y pruebas de intrusión desde el interior y el exterior de la compañía. Actividades incluidas

Las actividades apuntan a:

- Localizar los principales puntos de entrada de la plataforma de red corporativa.
- Identificación de las principales debilidades presentes en la tecnología de acceso y de transporte de los sistemas de información de misión crítica.
- Cuantificar de los puntos de acceso.
- Identificar los principales recursos Accesibles a través de cada punto de acceso.
- Validar las debilidades detectadas en las tecnologías, puntos de acceso y principales controles de la compañía.
- Ejecutar de un test de penetración/Ethical hacking a través de las debilidades encontradas que confirmara el factor de riesgo de la explotación del mismo como parte de un ataque real. (Será realizado con autorización expresa de la compañía).
- Test de penetración tipo: White Box.
- Valoración de las debilidades encontradas.
- Entrega de reporte de Evaluación de las principales Vulnerabilidades encontradas.

//

TEST RUN VULNERABILITY IN PUBLIC KEY INFRASTRUCTURE OF PONAL, ACCORDING TO THE FOLLOWING DEFINITIONS:

The contractor shall identify, quantify, validate and assess the main vulnerabilities in Technology PKI platform; like running a penetration test type White box to the main information systems and network services that are part of the PKI technology infrastructure in order to validate the identified weaknesses that could cause unmanageable level of risk and facilitate the engagement of corporate processes.

- Security Vulnerability Assessment Information regarding the logical access.
- Identification of technical vulnerabilities on servers in the organization.
- Conducting vulnerability assessment and penetration testing from inside and outside the company. activities included

The activities aim to:

- Locate the main points of entry into the corporate network platform.
- Identification of major weaknesses in access technology and transportation systems mission-critical information.
- Quantify the access points.
- Identify key resources Accessible through each access point.
- Validate the weaknesses identified in technologies, hotspots and main controls of the company.
- Run a penetration test / Ethical hacking through the weaknesses found to confirm the risk factor of the exploitation of it as part of a real attack. (It will be done with the express permission of the company).
- Penetration Test Type: White Box.
- Assessment of the weaknesses found.
- Delivery report Assessment of the main vulnerabilities found.
- The contractor shall deliver the definition of medium-term goals of the improvement plan established at least in a period of one (1) year and short-term established of at least six (6) months.
- The contractor shall perform and deliver the improvement plan (training, development of organizational assets, development of enabling organizational enablers for the management system projects, programs and portfolios) based on the results of the benchmarking, the initial diagnosis, the specific needs of the strategic direction, the action plans of the Office of Telematics and enhancement module OPM3.
- Should identify the best practices to develop in order to establish a project management office (PMO) in the entity.
- As a result, the contractor must submit an action plan, listing the best practices prioritized, referencing methodological tools associated with the organizational structure of the Office of Telematics.

Remediación de vulnerabilidades//Vulnerability Remediation

EJECUTAR LA AUDITORÍA DE TERCERA PARTE, SIGUIENDO LOS LINEAMIENTOS DE LA ISO/IEC 19011.
//RUN THE AUDIT OF THIRD PARTY FOLLOWING THE REQUIREMENTS OF THE ISO / IEC 19011.

El contratista realizará una auditoría de tercera parte, empleando auditores calificados y certificados de acuerdo a los requisitos exigidos por el ONAC, Requisito: Empresa de auditoría legalmente constituida en donde el objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de clave pública PKI. Reconocimiento web trust, auditores profesionales en la ingeniería de sistemas los cuales deben demostrar: 3 años de experiencia en auditoria de sistemas, 3 años de experiencia en ISO/IEC 27001 y 3 años de experiencia en infraestructura de llave pública (PKI), Competencia y experiencia certificada. Auditor con formación en ISO/IEC 17065 e ISO/IEC 27001.

//

The Contractor will conduct a third party audit, using qualified auditors and certified according to the requirements of the ONAC, Requirement: Company legally constituted audit where the object is included social services systems audit, information security and public Key Infrastructure PKI. Public recognition trust, professionals in systems engineering auditors who must prove: 3 years experience in auditing systems, 3 years experience in ISO / IEC 27001 and 3 years experience in public key infrastructure (PKI), Competition and certified experience. Auditor training ISO / IEC 17065 and ISO / IEC 27001

ENTREGAR Y ATENDER LA AUDITORÍA DE ACREDITACIÓN ANTE EL ORGANISMO NACIONAL DE ACREDITACIÓN, ONAC. //HIRE AND MEET THE AUDIT OF ACCREDITATION TO THE NATIONAL ACCREDITATION BODY, ONAC.

El contratista preparará toda la documentación exigida por ONAC; el contratista debe suministrar los servicios de auditoria y acreditación con ONAC y atender la visita de acreditación, siguiendo los lineamientos requeridos y consignados en las reglas de acreditación: R-AC 01 al R-AC 04, así como la diligencia de F-SOL (Formulario de Solicitud). //HIRE AND MEET THE AUDIT OF ACCREDITATION TO THE NATIONAL ACCREDITATION BODY, ONAC.

the contractor shall prepare all documentation required by ONAC; the contractor must hire the services of auditing and accreditation with ONAC and meet the accreditation visit, following the guidelines required are indicated in the rules of accreditation: R-01 to R AC-AC 04 and the diligence of F-SOL (Application Form).

GENERALIDADES // GENERAL

La implementación de los requerimientos mínimos se desarrollaran en la oficina de telemática (en sitio). // The implementation of the minimum requirements will be held in the office of telematics (on site)

CAPACITACIÓN (DEBE SER EN IDIOMA ESPAÑOL)// TRAINING (MUST BE IN SPANISH LANGUAGE)

El contratista deberá entregar en la propuesta el plan de capacitación, en el que se describa como desarrollara cada una de las actividades de los entregables.

El Contratista debe capacitar a quince (15) funcionarios como mínimo en nivel técnico para implementación, manejo, y operación de la toda la implementacion, a quien designe el supervisor del contrato.

Duración mínima de cuarenta (40) horas. El contratista garantizará la locación y material adecuado, como manuales para llevar a cabo la capacitación.

Los gastos que llegase a generarse con ocasión a las diferentes capacitaciones correrán a cargo del contratista.// The contractor shall deliver the proposed training plan, which is described as develop each of the activities of the deliverables.

The Contractor shall train fifteen (15) officials in at least the technical level to implementation, management, and operation of the entire implementation, which is at the discretion of the supervisor the place and date of the training.

Minimum period of forty (40) hours. The contractor shall ensure the location and suitable material, such as manuals to conduct the training.

The expenses were to be generated during the different trainings borne by the contractor.

COSTO DE LA CAPACITACIÓN // COST OF TRAINING

El valor de la capacitación ofrecida se debe incluir en el costo total del proyecto. El contratista con aprobación del supervisor determinará las fechas y el lugar para su realización.

Se debe entregar el cronograma de capacitación clasificado por temas y por perfiles.// The value of the offered training should be included in the total project cost. The contractor with supervisory approval shall determine the dates and venue for its realization.

Should deliver the training schedule by topic and profiles.

El contratista entregara: Plataforma PKI funcionando con equipo TSA, integracion con GECOP firmando documentos con sus respectivos certificados de los usuarios y toda la plataforma tecnologica correspondiente a la PKI configurada para acreditación (CEA-CDF que establece: Requisitos normativos, requisitos reglamentarios, requisitos técnicos, requisitos de aseguramiento) en un periodo de seis (6) meses. //The contractor will deliver: PKI platform running team TSA, integration with GECOP signing documents with their certificates of users and all relevant PKI technology platform configured for Accreditation (CEA-CDF which states: regulatory requirements, regulatory requirements, technical requirements , assurance requirements) over a period of six (6) months.

CERTIFICADO DE CAPACITACIÓN. // CERTIFICATE OF TRAINING

El contratista deberá entregar un certificado a cada uno de los funcionarios, al igual que elaborar acta de cada una de ellas, las cuales serán entregadas en original al supervisor del contrato.// The contractor shall deliver a certificate to each of the officers, as well as prepare minutes of each training, which will be delivered in the original contract supervisor.

SOLUCIÓN PROPUESTA

El contratista debe garantizar que la oferta propuesta para la implementación del equipo de TSA y software que integre el GECOP y la entrega de certificados para la firma digital de los usuarios cumpla con los requerimientos de acreditacion de la ONAC Y se adapte a las especificaciones mininas solicitadas por la Policía Nacional.// The contractor must ensure that the offer for the implementation team TSA and software that integrates GECOP and delivery of certificates for digital signature user meets the requirements of accreditation of the ONAC and suits the mininas specifications you requested Naciona by Police.

INCLUSIÓN DE FALTANTES//INCLUSION OF MISSING

Si durante el desarrollo del proyecto y hasta la prueba de aceptación por parte del supervisor del contrato se encuentra que no se incluyeron elementos, documentación o servicios indispensables para el correcto funcionamiento de la propuesta para la implementación del equipo de TSA y software que integre el GECOP y la entrega de certificados para la firma digital de los usuarios que cumpla con los requerimientos de acreditacion de la ONAC el contratista deberá incluirlo, suministrarlo, y ponerlo en funcionamiento sin costo adicional.mininas solicitadas por la Policía Nacional. // If you are not elements,

documentation or services essential to the proper functioning of the proposal to implement the TSA equipment and software that integrates included in the project and to test acceptance by the supervisor of the contract GECOP and delivery of digital signature certificates for users who meets the accreditation requirements of the ONAC the contractor shall include, deliver it, and put into operation without additional.mininas cost Naciona requested by the Police.

CONFIDENCIAL Y ACUERDOS DE CONFIABILIDAD // CONFIDENTIALITY AGREEMENTS AND RELIABILITY

El contratista (todos los funcionarios que participen en la implementación y ejecución del proyecto) deberán diligenciar los formatos CONFIDENCIAL Y ACUERDOS DE CONFIABILIDAD una vez se firme el contrato.//The contractor (all staff involved in the implementation and execution of the project) must fill out the CONFIDENTIAL AND AGREEMENTS OF RELIABILITY forms once the contract is signed.

EJECUTAR LA AUDITORÍA DE TERCERA PARTE, SIGUIENDO LOS LINEAMIENTOS DE LA ISO/IEC 19011.

El contratista realizará una auditoría de tercera parte, empleando auditores calificados y certificados de acuerdo a los requisitos exigidos por el ONAC,Requisito: Empresa de auditoría legalmente constituida en donde el objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de clave pública PKI. Reconocimiento web trust, auditores profesionales en la ingeniería de sistemas los cuales deben demostrar: 3 años de experiencia en auditoria de sistemas, 3 años de experiencia en ISO/IEC 27001 y 3 años de experiencia en infraestructura de llave pública (PKI), Competencia y experiencia certificada. Auditor con formación en ISO/IEC 17065 e ISO/IEC 27001.

//RUN THE AUDIT OF THIRD PARTY FOLLOWING THE REQUIREMENTS OF THE ISO / IEC 19011.

The Contractor will conduct a third party audit, using qualified auditors and certified according to the requirements of the ONAC, Requirement: Company legally constituted audit where the object is included social services systems audit, information security and public Key Infrastructure PKI. Public recognition trust, professionals in systems engineering auditors who must prove: 3 years experience in auditing systems, 3 years experience in ISO / IEC 27001 and 3 years experience in public key infrastructure (PKI), Competition and certified experience. Auditor training ISO / IEC 17065 and ISO / IEC 27001.

El contratista respondera por la Ejecución AUDITORÍA DE ACREDITACIÓN ANTE ONAC entregable certificado de acreditación de la PKI de la Policia Nacional por parte de ONAC. // The contractor will respond by AUDIT OF ACCREDITATION TO ONAC deliverable Execution accreditation certificate PKI National Police by ONAC.